



Pegasus scandal shows risk of Israel's spy-tech diplomacy: experts

Issued on: 19/07/2021

Jerusalem (AFP)

Reports that Israel-made Pegasus spyware has been used to monitor activists, journalists and politicians around the world highlight the diplomatic risks of nurturing and exporting "oppressive technology", experts warned Monday.

Private Israeli firm NSO Group has denied media reports its Pegasus software is linked to the mass surveillance of journalists and rights defenders, and insisted that all sales of its technology are approved by Israel's defence ministry.

Founded in 2010 and based in Herzliya, north of Tel Aviv, NSO says it develops tools that allow governments to pursue criminals who might evade authorities through encrypted communications.

But the Washington Post, the Guardian, Le Monde and other news outlets that collaborated on an investigation reported on a leaked list of up to 50,000 phone numbers believed to have been identified as people of interest by clients of NSO since 2016, not all of whom were hacked.

NSO spokesman Oded HersHKovitz told Israel's Army Radio the list of phone numbers was "not connected" to NSO, but rather to other companies and open-source software.

"We didn't receive until today a bit of evidence that on this list someone indeed was attacked by the Pegasus system," HersHKovitz said.

The software enables phones to be infiltrated and tracked, with the microphone and camera activated remotely to monitor the user.

- 'Incubator for oppressive technology' -

Israeli experts recalled the country's long history of using the export of cutting edge weaponry to foster diplomatic relations, but warned that burgeoning sales of advanced surveillance systems could cause more harm than benefit.

"Israeli weapons exports helped the country forge all kind of ties," said **Yoel Guzansky** from the **Institute for National Security Studies** in Tel Aviv.

He cited quiet ties in the Middle East, Africa and Asia built through the weapons trade.

"Sometimes the damage is bigger than the benefit," **Guzansky** told AFP. "Israel might be seen as someone who helps autocratic regimes suppress civil society."

Jonathan Klinger, an Israeli cyber law attorney and privacy specialist, agreed, charging that "Israel is an incubator for oppressive technology".

But he said "a big problem" is that NSO's reported exports do not amount to a crime under Israeli law.

Klinger criticised what he called an "unfortunate business model," helped by Israel's readiness to test new surveillance systems on Palestinians in the occupied West Bank, Gaza and annexed east Jerusalem.

But the market is substantial, he added, because "there's a limited number of liberal democracies, and there's more dictatorships worldwide."

NSO's Hershkovitz told Army Radio the firm is a "Zionist company that operates only from Israel", and only with approval from the defence ministry.

Last month, NSO said it considers the "past human rights performance and governance standards" of its clients.

Contracts require customers to "respect human rights", including "rights to privacy and freedom of expression," NSO said.

As a result, NSO had blacklisted 55 countries and rejected more than \$300 million in potential "opportunities".

In 12 complaints it considered about the use of its product last year, NSO said one had resulted in termination of a contract.

- 'Dark side' -

The leaked list of potential hacking targets was obtained by rights group Amnesty International and Forbidden Stories, a Paris-based media non-profit organisation.

Israel's defence ministry said it did not have access to information gathered by NSO's clients.

Israel "approves the export of cyber products exclusively to governmental entities, for lawful use, and only for the purpose of preventing and investigating crime and counter terrorism," it said.

NSO does not reveal which governments buy its products.

But the reported list of targeted phone numbers were clustered in 10 countries including Azerbaijan, Bahrain, Morocco, Saudi Arabia and the United Arab Emirates.

Israel reached historic normalisation agreements with Bahrain, Morocco, Sudan and the UAE last year.

Guzansky said access to surveillance software was not the only reason for the deepening ties with Arab nations. "But of course, it helps," he said.

Israeli concerns about NSO technology are not new.

In 2019, then-head of the Israel Innovation Authority Aharon Aharon said he believed the firm was part of "the dark side" of technological advancement.

Israeli cybersecurity expert May Brooks-Kempler said that despite the outcry over NSO's tools being used to possibly abuse rights, she did not think the company faced an existential threat.

"The customers of a company like that are government agencies," she said.

"It may mean a bit more scrutiny by the [Israeli] ministry of defence, but at the end of the day, tyrants don't care about global news outlets."

<https://www.france24.com/en/live-news/20210719-pegasus-scandal-shows-risk-of-israel-s-spy-tech-diplomacy-experts>